UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/847,813	05/01/2001	Curt Wohlgemuth	OMNI0008	6351

7590 07/13/2006

PERKINS COIE LLP
ATTN: Mr. Brian R. Coleman
101 Jefferson Drive
Menlo Park, CA 94025

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 07/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/847,813	WOHLGEMUTH ET AL.	
	Examiner	Art Unit	
	Benjamin E Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,10-12,19,25 and 31-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,10-12,19,25 and 31-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 10/6/03
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 16 May 2006 amends claims 31, 33, 34, 37, 42, and 44. Applicant's amendment has been fully considered and is entered.

Response to Arguments

2. Applicant's arguments filed 16 May 2006 have been fully considered but they are not persuasive. Applicant's argument that Safadi does not disclose streaming software is not persuasive because Safadi discloses providing impulse purchasing of services over a communication network (Abstract). Such services can include streaming media (Abstract). The media can include games (Col. 1, lines 38-39). These games would be software application executables.

3. Applicant appears to suggest that Safadi is not concerned with protecting the services of Safadi from piracy. This argument is not persuasive because Safadi discloses that in order to provide the mentioned services, security must be implemented (Col. 1, lines 41-42). Security is provided using conditional access techniques (Col. 1, lines 43-44). Conditional access techniques work by authenticating the requestor, which meets the limitation of determining whether ran originating process that is making said requests for access is a trusted process. Determining whether a section of said streaming application program files that is being requested is a critical section that requires protection from piracy is meet inherently in the system because the security mechanism provides security for all of the media or services that require security. Safadi uses a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17) to determine whether conditional access to the services or media will be granted. This meets the limitation of a history

of previous requests for access made by an originating process because the credit amount changes after each authorized use. Once the subscriber's credit amount has expired, conditional access will no longer be granted. Piracy is merely the unauthorized use of protected material, and Safadi protects services and media from piracy by ensuring that payment is made for the use of those services and media. The fact that the term 'piracy' is absent from the text of Safadi is irrelevant because the claim limitations are meet because of the structural and functional equivalence of Safadi.

4. Applicant makes numerous similar arguments with respect to Safadi and other claims. Those arguments are fully addressed in view of the responses above.

5. Applicant's arguments with respect to the meaning of "streaming-enabled" and the Vahalia reference have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Rothman, U.S. Publication 2001/0044851, and Abdelnur, U.S. Patent No. 6,212,640, which is incorporated into Rothman by reference.

Claim Objections

6. Claim 35 is objected to because of the following informalities: line 3 recites "form" instead of "from". Appropriate correction is required.

Claim Rejections - 35 USC § 101

7. Claims 38, 39 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 38 and 39 are directed towards one or more propagated data signals, which are reasonably interpreted as a form of energy that is not capably of causing functional change in a computer. See, e.g., Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760.

"Functional descriptive material consists of data structures and computer programs which impart functionality when employed as a computer component." Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility Annex IV, Oct. 26, 2005, at http://www.uspto.gov/web/offices/pac/dapp/opla/preognotice/guidelines101_20051026.pdf, 1300 OG 142 (Nov. 22, 2005).

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 2, 11, 19, 25 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 2, 11, 19, 25, the phrase "such as" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. Claims 1-3, 10-12, 19, 25, 31-33, 35, 36, 38-41, 43 are rejected under 35 U.S.C. 102(e) as being anticipated by Rothman, U.S. Publication 2001/0044851, which incorporates Abdelnur, U.S. Patent No. 6,212,640, by reference. Referring to claim 1, Rothman discloses a system and method for delivering streaming media wherein a network file system is utilized as the underlying network configuration to stream media to end users ([0060] & [0062]), which meets the limitation of providing a network file system on a client, wherein said network file system handles and forwards requests from streaming-enabled local processes on said client that are directed at streaming application program files located on said server. The Abdelnur reference is incorporated into Rothman by reference to disclose the streaming system and method (Rothman [0062]). The NFS server finds the file for which the request was made and verifies whether the requesting application has permission to access the file (Abdelnur Col. 7, lines 48-52), which meets the limitation of wherein said network file system examines said requests, and either grants or denies each of said requests depending on whether the request is justifiable from a security perspective. One security parameter would allow the requesting application access to the requested file if the application is a trusted application (Abdelnur Col. 8, lines 43-52), which meets the limitation of granting or denying each of said requests depending on whether the request is justifiable from a security perspective by using the nature of the originating streaming-enabled process. If permission is granted, NFS server returns a file handle to NFS client through the communication link, so that the client can access the file system (Abdelnur Col. 7, lines 52-54), which meets the limitation of providing a network redirector component of said network file system, and wherein said network redirector component makes visible to said network file system, a path that represents the server where said streaming application program files are

stored. The media meets the limitation of application program files because the media is streamed to the user terminal for execution using a player application (Rothman [0006]).

Referring to claim 2, Abdelnur discloses that each file accessed on the remote server is identified by a unique file handle by which NFS clients refer to files on an NFS server (Col. 6, lines 65-67). Handles are globally unique and are passed in operations, such as read and write, that reference a file (Col. 6, line 67 – Col. 7, line 2), which meets the limitation of said network file system registers dispatch routines with the client operating system that handle common file operations such as open, read, write and close, wherein a dispatch routine examines a file request and decides whether to grant or deny said file request, and wherein if said file request is granted then said dispatch routine forwards said file request to said server and sends back said server's response to said client operating system.

Referring to claim 3, Abdelnur the NFS server finds the file for which the request was made and verifies whether the requesting application has permission to access the file (Abdelnur Col. 7, lines 48-52). Each file accessed on the remote server is identified by a unique file handle by which NFS clients refer to files on an NFS server (Col. 6, lines 65-67). Handles are globally unique and are passed in operations, such as read and write, that reference a file (Col. 6, line 67 – Col. 7, line 2), which meets the limitation of when a local streaming-enabled process on said client makes a file request for a streaming application program file on said server, said client operating system calls a dispatch routine with said file request.

Referring to claim 10, Rothman discloses a system and method for delivering streaming media wherein a network file system is utilized as the underlying network configuration to stream media to end users ([0060] & [0062]), which meets the limitation of providing a network

file system on a client, wherein said network file system handles and forwards requests from streaming-enabled local processes on said client that are directed at streaming application program files located on said server. The Abdelnur reference is incorporated into Rothman by reference to disclose the streaming system and method (Rothman [0062]). The NFS server finds the file for which the request was made and verifies whether the requesting application has permission to access the file (Abdelnur Col. 7, lines 48-52), which meets the limitation of wherein said network file system examines said requests, and either grants or denies each of said requests depending on whether the request is justifiable from a security perspective. One security parameter would allow the requesting application access to the requested file if the application is a trusted application (Abdelnur Col. 8, lines 43-52), which meets the limitation of granting or denying each of said requests depending on whether the request is justifiable from a security perspective by using the nature of the originating streaming-enabled process. If permission is granted, NFS server returns a file handle to NFS client through the communication link, so that the client can access the file system (Abdelnur Col. 7, lines 52-54), which meets the limitation of providing a network redirector component of said network file system, and wherein said network redirector component makes visible to said network file system, a path that represents the server where said streaming application program files are stored. The media meets the limitation of application program files because the media is streamed to the user terminal for execution using a player application (Rothman [0006]).

Referring to claim 11, Abdelnur discloses that each file accessed on the remote server is identified by a unique file handle by which NFS clients refer to files on an NFS server (Col. 6, lines 65-67). Handles are globally unique and are passed in operations, such as read and write,

that reference a file (Col. 6, line 67 – Col. 7, line 2), which meets the limitation of said network file system registers dispatch routines with the client operating system that handle common file operations such as open, read, write and close, wherein a dispatch routine examines a file request and decides whether to grant or deny said file request, and wherein if said file request is granted then said dispatch routine forwards said file request to said server and sends back said server's response to said client operating system.

Referring to claim 12, Abdelnur the NFS server finds the file for which the request was made and verifies whether the requesting application has permission to access the file (Abdelnur Col. 7, lines 48-52). Each file accessed on the remote server is identified by a unique file handle by which NFS clients refer to files on an NFS server (Col. 6, lines 65-67). Handles are globally unique and are passed in operations, such as read and write, that reference a file (Col. 6, line 67 – Col. 7, line 2), which meets the limitation of when a local streaming-enabled process on said client makes a file request for a streaming application program file on said server, said client operating system calls a dispatch routine with said file request.

Referring to claim 19, Rothman discloses a system and method for delivering streaming media wherein a network file system is utilized as the underlying network configuration to stream media to end users ([0060] & [0062]), which meets the limitation of providing a file system on a client, wherein said file system handles and forwards requests from streaming-enabled local processes on said client. The Abdelnur reference is incorporated into Rothman by reference to disclose the streaming system and method (Rothman [0062]). The NFS server finds the file for which the request was made and verifies whether the requesting application has permission to access the file (Abdelnur Col. 7, lines 48-52), which meets the limitation of

wherein said file system examines said requests, and either grants or denies each of said requests depending on whether the request is justifiable from a security perspective. One security parameter would allow the requesting application access to the requested file if the application is a trusted application (Abdelnur Col. 8, lines 43-52), which meets the limitation of granting or denying each of said requests depending on whether the request is justifiable from a security perspective by using the nature of the originating streaming-enabled process. If permission is granted, NFS server returns a file handle to NFS client through the communication link, so that the client can access the file system (Abdelnur Col. 7, lines 52-54). Each file accessed on the remote server is identified by a unique file handle by which NFS clients refer to files on an NFS server (Col. 6, lines 65-67). Handles are globally unique and are passed in operations, such as read and write, that reference a file (Col. 6, line 67 – Col. 7, line 2), which meets the limitation of said file system registers dispatch routines with the client operating system that handle common file operations such as open, read, write and close, wherein a dispatch routine examines a file request and decides whether to grant or deny said file request, and wherein if said file request is granted then said dispatch routine allows the requested operation to proceed. The media meets the limitation of application program files because the media is streamed to the user terminal for execution using a player application (Rothman [0006]).

Referring to claim 25, Rothman discloses a system and method for delivering streaming media wherein a network file system is utilized as the underlying network configuration to stream media to end users ([0060] & [0062]), which meets the limitation of providing a file system on a client, wherein said file system handles and forwards requests from streaming-enabled local processes on said client. The Abdelnur reference is incorporated into Rothman by

reference to disclose the streaming system and method (Rothman [0062]). The NFS server finds the file for which the request was made and verifies whether the requesting application has permission to access the file (Abdelnur Col. 7, lines 48-52), which meets the limitation of wherein said file system examines said requests, and either grants or denies each of said requests depending on whether the request is justifiable from a security perspective. One security parameter would allow the requesting application access to the requested file if the application is a trusted application (Abdelnur Col. 8, lines 43-52), which meets the limitation of granting or denying each of said requests depending on whether the request is justifiable from a security perspective by using the nature of the originating streaming-enabled process. If permission is granted, NFS server returns a file handle to NFS client through the communication link, so that the client can access the file system (Abdelnur Col. 7, lines 52-54). Each file accessed on the remote server is identified by a unique file handle by which NFS clients refer to files on an NFS server (Col. 6, lines 65-67). Handles are globally unique and are passed in operations, such as read and write, that reference a file (Col. 6, line 67 – Col. 7, line 2), which meets the limitation of said file system registers dispatch routines with the client operating system that handle common file operations such as open, read, write and close, wherein a dispatch routine examines a file request and decides whether to grant or deny said file request, and wherein if said file request is granted then said dispatch routine allows the requested operation to proceed. The media meets the limitation of application program files because the media is streamed to the user terminal for execution using a player application (Rothman [0006]).

Referring to claim 31, Rothman discloses a system and method for delivering streaming media wherein a network file system is utilized as the underlying network configuration to

stream media to end users ([0060] & [0062] & Figure 2), which meets the limitation of using a first computer to serve streaming application program files to a second computer for streaming execution. The Abdelnur reference is incorporated into Rothman by reference to disclose the streaming system and method (Rothman [0062]). The NFS server finds the file for which the request was made and verifies whether the requesting application has permission to access the file (Abdelnur Col. 7, lines 48-52), which meets the limitation of using a filtering mechanism that is associated with said second computer for filtering requests for access to said streaming application program files, said filtering mechanism determines whether to grant requests for access to said streaming application program files. One security parameter would allow the requesting application access to the requested file if the application is a trusted application (Abdelnur Col. 8, lines 43-52), which meets the limitation of granting requests for access to said streaming application program files by determining a nature of an originating process that is making said requests for access. The media meets the limitation of application program files because the media is streamed to the user terminal for execution using a player application (Rothman [0006]).

Referring to claim 32, The Abdelnur reference is incorporated into Rothman by reference to disclose the streaming system and method (Rothman [0062]). The NFS server finds the file for which the request was made and verifies whether the requesting application has permission to access the file (Abdelnur Col. 7, lines 48-52). One security parameter would allow the requesting application access to the requested file if the application is a trusted application (Abdelnur Col. 8, lines 43-52), which meets the limitation of providing information relating to one or more remote locations where streaming application program files are stored, determining whether an

originating process that is making said requests for access is a trusted process. Abdelnur discloses that the network file system authenticates the requesting applications to determine if they can be trusted to access protected files (Abdelnur Col. 7, line 49 – Col. 8, line 7). This meets the limitation of determining a pre-determined pattern of piracy and determining whether the application program files is a critical section that requires protection from piracy because Rothman discloses that the media files are commercial content governed by the United States by the DMCA (Rothman [0097]). Therefore, the files mentioned have been predetermined as critical files that require protection from privacy and security measures implemented within the disclosed system preemptive measures against predetermined patterns of piracy. The media meets the limitation of application program files because the media is streamed to the user terminal for execution using a player application (Rothman [0006]).

Referring to claim 33, The Abdelnur reference is incorporated into Rothman by reference to disclose the streaming system and method (Rothman [0062]). The NFS server finds the file for which the request was made and verifies whether the requesting application has permission to access the file (Abdelnur Col. 7, lines 48-52). One security parameter would allow the requesting application access to the requested file if the application is a trusted application (Abdelnur Col. 8, lines 43-52), which meets the limitation of providing information relating to one or more remote locations where streaming application program files are stored, determining whether an originating process that is making said requests for access is a trusted process. If permission is granted, NFS server returns a file handle to NFS client through the communication link, so that the client can access the file system (Abdelnur Col. 7, lines 52-54). Each file accessed on the remote server is identified by a unique file handle by which NFS clients refer to files on an NFS

server (Col. 6, lines 65-67). Handles are globally unique and are passed in operations, such as read and write, that reference a file (Col. 6, line 67 – Col. 7, line 2), which meets the limitation of using dispatch routines for examining a request for access to said streaming application program files. Abdelnur discloses that the network file system authenticates the requesting applications to determine if they can be trusted to access protected files (Abdelnur Col. 7, line 49 – Col. 8, line 7). This meets the limitation of after examining said request and if it is determined that a history of previous requests for access made by said originating process lacks a predetermined pattern of piracy, then forwarding said request to a corresponding remote server that is responsible for serving said streaming application program files because Rothman discloses that the media files are commercial content governed by the United States by the DMCA (Rothman [0097]). Therefore, the security measures implemented within the disclosed system preemptive measures against predetermined patterns of piracy. The media meets the limitation of application program files because the media is streamed to the user terminal for execution using a player application (Rothman [0006]).

Referring to claim 35, Rothman discloses a system and method for delivering streaming media wherein a network file system is utilized as the underlying network configuration to stream media to end users ([0060] & [0062]). The Abdelnur reference is incorporated into Rothman by reference to disclose the streaming system and method (Rothman [0062]). The NFS server finds the file for which the request was made and verifies whether the requesting application has permission to access the file (Abdelnur Col. 7, lines 48-52), which meets the limitation of a processing device for processing a request for access to streaming application program files stored on at least one server system that is remote from said processing device.

One security parameter would allow the requesting application access to the requested file if the application is a trusted application (Abdelnur Col. 8, lines 43-52). If permission is granted, NFS server returns a file handle to NFS client through the communication link, so that the client can access the file system (Abdelnur Col. 7, lines 52-54), which meets the limitation of a redirector component that is associated with said processing device for informing said processing device of one or more locations in which said streaming application program files are stored. The media meets the limitation of application program files because the media is streamed to the user terminal for execution using a player application (Rothman [0006]). Abdelnur discloses that the network file system authenticates the requesting applications to determine if they can be trusted to access protected files (Abdelnur Col. 7, line 49 – Col. 8, line 7). This meets the limitation of determining a pre-determined pattern of piracy and determining whether the application program files is a critical section that requires protection from piracy because Rothman discloses that the media files are commercial content governed by the United States by the DMCA (Rothman [0097]). Therefore, the files mentioned have been predetermined as critical files that require protection from privacy and security measures implemented within the disclosed system preemptive measures against predetermined patterns of piracy. The media meets the limitation of application program files because the media is streamed to the user terminal for execution using a player application (Rothman [0006]).

Referring to claim 36, Rothman discloses a system and method for delivering streaming media wherein a network file system is utilized as the underlying network configuration to stream media to end users ([0060] & [0062]). The Abdelnur reference is incorporated into Rothman by reference to disclose the streaming system and method (Rothman [0062]). The NFS

server finds the file for which the request was made and verifies whether the requesting application has permission to access the file (Abdelnur Col. 7, lines 48-52), which meets the limitation of a processing means for processing requests for access to streaming application program files stored remotely from said processing means. One security parameter would allow the requesting application access to the requested file if the application is a trusted application (Abdelnur Col. 8, lines 43-52). If permission is granted, NFS server returns a file handle to NFS client through the communication link, so that the client can access the file system (Abdelnur Col. 7, lines 52-54), which meets the limitation of a redirection means for revealing one or more locations in which said streaming application program files are stored. The media meets the limitation of application program files because the media is streamed to the user terminal for execution using a player application (Rothman [0006]). Abdelnur discloses that the network file system authenticates the requesting applications to determine if they can be trusted to access protected files (Abdelnur Col. 7, line 49 – Col. 8, line 7), which meets the limitation of determining means for determining whether to grant requests for access to said streaming application program files if the originating process that is making said requests for access is a trusted process. This meets the limitation of determining a pre-determined pattern of piracy and determining whether the application program files is a critical section that requires protection from piracy because Rothman discloses that the media files are commercial content governed by the United States by the DMCA (Rothman [0097]). Therefore, the files mentioned have been predetermined as critical files that require protection from privacy and security measures implemented within the disclosed system preemptive measures against predetermined patterns of

piracy. The media meets the limitation of application program files because the media is streamed to the user terminal for execution using a player application (Rothman [0006]).

Referring to claim 38, The Abdelnur reference is incorporated into Rothman by reference to disclose the streaming system and method (Rothman [0062]). The NFS server finds the file for which the request was made and verifies whether the requesting application has permission to access the file (Abdelnur Col. 7, lines 48-52). One security parameter would allow the requesting application access to the requested file if the application is a trusted application (Abdelnur Col. 8, lines 43-52), which meets the limitation of providing information relating to one or more remote locations where streaming application program files are stored, determining whether an originating process that is making said requests for access is a trusted process. Abdelnur discloses that the network file system authenticates the requesting applications to determine if they can be trusted to access protected files (Abdelnur Col. 7, line 49 – Col. 8, line 7). This meets the limitation of determining a pre-determined pattern of piracy and determining whether the application program files is a critical section that requires protection from piracy because Rothman discloses that the media files are commercial content governed by the United States by the DMCA (Rothman [0097]). Therefore, the files mentioned have been predetermined as critical files that require protection from privacy and security measures implemented within the disclosed system preemptive measures against predetermined patterns of piracy. The media meets the limitation of application program files because the media is streamed to the user terminal for execution using a player application (Rothman [0006]).

Referring to claim 39, The Abdelnur reference is incorporated into Rothman by reference to disclose the streaming system and method (Rothman [0062]). The NFS server finds the file

for which the request was made and verifies whether the requesting application has permission to access the file (Abdelnur Col. 7, lines 48-52). One security parameter would allow the requesting application access to the requested file if the application is a trusted application (Abdelnur Col. 8, lines 43-52), which meets the limitation of providing information relating to one or more remote locations where streaming application program files are stored, determining whether an originating process that is making said requests for access is a trusted process. If permission is granted, NFS server returns a file handle to NFS client through the communication link, so that the client can access the file system (Abdelnur Col. 7, lines 52-54). Each file accessed on the remote server is identified by a unique file handle by which NFS clients refer to files on an NFS server (Col. 6, lines 65-67). Handles are globally unique and are passed in operations, such as read and write, that reference a file (Col. 6, line 67 – Col. 7, line 2), which meets the limitation of using dispatch routines for examining a request for access to said streaming application program files. Abdelnur discloses that the network file system authenticates the requesting applications to determine if they can be trusted to access protected files (Abdelnur Col. 7, line 49 – Col. 8, line 7). This meets the limitation of after examining said request and if it is determined that a history of previous requests for access made by said originating process lacks a predetermined pattern of piracy, then forwarding said request to a corresponding remote server that is responsible for serving said streaming application program files because Rothman discloses that the media files are commercial content governed by the United States by the DMCA (Rothman [0097]). Therefore, the security measures implemented within the disclosed system preemptive measures against predetermined patterns of piracy. The media meets the limitation of application program

files because the media is streamed to the user terminal for execution using a player application (Rothman [0006]).

Referring to claim 40, The Abdelnur reference is incorporated into Rothman by reference to disclose the streaming system and method (Rothman [0062]). The NFS server finds the file for which the request was made and verifies whether the requesting application has permission to access the file (Abdelnur Col. 7, lines 48-52). One security parameter would allow the requesting application access to the requested file if the application is a trusted application (Abdelnur Col. 8, lines 43-52), which meets the limitation of providing information relating to one or more remote locations where streaming application program files are stored, determining whether an originating process that is making said requests for access is a trusted process. Abdelnur discloses that the network file system authenticates the requesting applications to determine if they can be trusted to access protected files (Abdelnur Col. 7, line 49 – Col. 8, line 7). This meets the limitation of determining a pre-determined pattern of piracy and determining whether the application program files is a critical section that requires protection from piracy because Rothman discloses that the media files are commercial content governed by the United States by the DMCA (Rothman [0097]). Therefore, the files mentioned have been predetermined as critical files that require protection from privacy and security measures implemented within the disclosed system preemptive measures against predetermined patterns of piracy. The media meets the limitation of application program files because the media is streamed to the user terminal for execution using a player application (Rothman [0006]).

Referring to claim 41, Rothman discloses a system and method for delivering streaming media wherein a network file system is utilized as the underlying network configuration to

stream media to end users ([0060] & [0062]), which meets the limitation of a means for providing location information to a local computing system of streaming application program files that are stored on one or more remote locations. The Abdelnur reference is incorporated into Rothman by reference to disclose the streaming system and method (Rothman [0062]). The NFS server finds the file for which the request was made and verifies whether the requesting application has permission to access the file (Abdelnur Col. 7, lines 48-52), which meets the limitation of a means for examining requests for access to said streaming application program files. One security parameter would allow the requesting application access to the requested file if the application is a trusted application (Abdelnur Col. 8, lines 43-52). If permission is granted, NFS server returns a file handle to NFS client through the communication link, so that the client can access the file system (Abdelnur Col. 7, lines 52-54), which meets the limitation of a means for forwarding said requests to a corresponding server that is responsible for serving said streaming application program files if said requests are granted. The media meets the limitation of application program files because the media is streamed to the user terminal for execution using a player application (Rothman [0006]). Abdelnur discloses that the network file system authenticates the requesting applications to determine if they can be trusted to access protected files (Abdelnur Col. 7, line 49 – Col. 8, line 7), which meets the limitation of a means for determining whether said requests can be granted on whether an originating process that is making said requests for access is a trusted process. This meets the limitation of determining a pre-determined pattern of piracy and determining whether the application program files is a critical section that requires protection from piracy because Rothman discloses that the media files are commercial content governed by the United States by the DMCA (Rothman [0097]).

Therefore, the files mentioned have been predetermined as critical files that require protection from privacy and security measures implemented within the disclosed system preemptive measures against predetermined patterns of piracy. The media meets the limitation of application program files because the media is streamed to the user terminal for execution using a player application (Rothman [0006]).

Referring to claim 43, Rothman discloses a system and method for delivering streaming media wherein a network file system is utilized as the underlying network configuration to stream media to end users ([0060] & [0062]), which meets the limitation of providing information relating to one or more remote locations streaming application program files that are stored. The Abdelnur reference is incorporated into Rothman by reference to disclose the streaming system and method (Rothman [0062]). The NFS server finds the file for which the request was made and verifies whether the requesting application has permission to access the file (Abdelnur Col. 7, lines 48-52), which meets the limitation of receiving a request from a computer process for access to said streaming application program files. One security parameter would allow the requesting application access to the requested file if the application is a trusted application (Abdelnur Col. 8, lines 43-52). Abdelnur discloses that the network file system authenticates the requesting applications to determine if they can be trusted to access protected files (Abdelnur Col. 7, line 49 – Col. 8, line 7). This meets the limitation of after examining said request and if it is determined that a history of previous requests for access made by said originating process lacks a predetermined pattern of piracy, then forwarding said request to a corresponding remote server that is responsible for serving said streaming application program files because Rothman discloses that the media files are commercial content governed by the

United States by the DMCA (Rothman [0097]). Therefore, the security measures implemented within the disclosed system preemptive measures against predetermined patterns of piracy. The media meets the limitation of application program files because the media is streamed to the user terminal for execution using a player application (Rothman [0006]).

12. Claims 31-42 are rejected under 35 U.S.C. 102(e) as being anticipated by Safadi, U.S. Patent No. 6,810,525. Referring to claim 31, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of using a first computer to serve said application program files to a second computer for execution, using a filtering mechanism that is associated with said second computer for filtering requests for access to said application program files, wherein said filtering mechanism determines whether to grant requests for access to said application program files by determining one or more criteria from a set of criteria comprising: a nature of an originating process that is making said requests for access, a history of previous requests for access made by said originating process, and a nature of a section of said application program files that is being requested. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 32, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of providing informaiton relating to one or more remote locations where said application program files are

stored, determining whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claims 33, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17). The client application of Safadi would meet the limitation of the dispatch routine that examines the file requests and decides whether to grant or deny said file request (Col. 2, lines 1-10, Col. 3, lines 11-17). which meets the limitation of providing information relating to one or more remote locations where said application program files are stored, using dispatch routines for examining a request for access to said application program files, after examining said request and if it is determined that an originating process that is making said request for access is a trusted process, or that a history of previous requests for access made by said originating process lacks a pre-determined pattern of piracy, and that a section of said application program files that is being requested is a non-critical section, then forwarding said request to a corresponding remote server that is responsible for serving said application program files. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 34, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of using a filtering mechanism on a client computer for filtering requests for access to said application program files, wherein said filtering mechanism determines whether to grant requests for access to said application program files by determining one or more criteria from a set of criteria comprising: a nature of an originating process that is making said requests for access, a history of previous requests for access made by said originating process, and a nature of a section of said application program files that is being requested. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of using a revealing mechanism to reveal to said client computer one or more remote locations on which said requested application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 35, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of a processing device for processing a request for access to said application program files stored on at least one server system that is remote from said processing device, wherein said processing device comprises a

component that determines whether to grant requests for access to said application program files based on: whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of a redirecting component that is associated with said processing device for informing said processing device of one or more locations in which said application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 36, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of processing means for processing a request for access to said application program files stored remotely from said processing means, wherein said processing means includes a determination whether to grant requests for access to said application program files based on: whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that

requires protection from piracy. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of a redirection means for revealing one or more locations in which said application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 37, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of a filtering means for filtering requests for access to said application program files stored remotely from said filtering means, wherein said filtering means includes an evaluation means for evaluating: an originating process that is making said requests for access, a history of previous requests for access made by said originating process, and a section of said application program files that is being requested. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of a redirection means for revealing one or more locations in which said requested application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 38, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be

authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of determining whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 39, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of using dispatch routines for examining a request for access to said application program files, after examining said request and if it is determined that an originating process that is making said request for access is a trusted process, and that a history of previous requests for access made by said originating process lacks a pre-determined pattern of piracy, and that a section of said application program files that is being requested is a non-critical section, then forwarding said request to a corresponding remote server that is responsible for serving said application program files. The

client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 40, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of determining whether an originating process that is making said request for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 41, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be

authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of a means for examining requests for access to said application program files, a means for determining whether said requests can be granted based on whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a predetermined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy, if said requests are granted then forwarding said requests to a corresponding server that is responsible for serving said application program files. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of a means for providing location information to a local computing system of said application program files that are stored on one or more remote locations. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 42, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of receiving a request from a computer process for access to said application program files, determining if said computer process that is making said request for access is a trusted process, if said computer process is a trusted process, then forwarding said request to a corresponding remote server that is

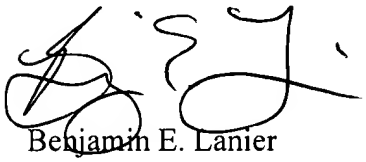
responsible for serving said application program files. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Benjamin E. Lanier